Technical Cybersecurity Intelligence Operations

Information Collection, Propaganda, Planting

Information Collection

Always needed, not always end goal

- Reconnaissance always needed

Sometimes targeted, sometimes not

- When not targeted, volume of data exfiltration an issue
- When targeted, not so much
- Encryption via standard ports (proxies can thwart)
- Sometimes multi-level encryption/obsfuscation strategies using multiple compression/encryption cycles

Propaganda

Very Common

- Facebook, Wikileaks, comment sections of news sites, data dumps (see: Wikileaks)
- Multiple APT groups working in this area
- In tandem with hacking ops

Unified across platforms

- Exfil information with additions, stories and phantom orgs on Social Media, Bot accounts on twitter for amplification

Information Planting

Not as common

- But don't rule it out
- Recently, planted info in stolen and released info as part of propaganda operations

Implantation more likely related to sabotage

Next up: Sabotage!